



# WLM-3501



Wireless ADSL2+ Modem Router

## User Manual

*Version: 1.0*

# Table of Contents

---

<b>INTRODUCTION.....</b>	<b>4</b>
<b>1 KEY FEATURES.....</b>	<b>5</b>
<b>2 PACKAGE CONTENTS .....</b>	<b>6</b>
<b>3 CAUTIONS .....</b>	<b>7</b>
<b>4 PRODUCT LAYOUT .....</b>	<b>8</b>
BACK LABEL	9
<b>5 SYSTEM REQUIREMENTS .....</b>	<b>10</b>
<b>6 WLM-3501 PLACEMENT .....</b>	<b>10</b>
<b>7 SETUP LAN, WAN.....</b>	<b>10</b>
<b>8 PC NETWORK ADAPTER SETUP .....</b>	<b>11</b>
WINDOWS XP	11
WINDOWS VISTA/WINDOWS 7	12
<b>9 BRING UP THE WLM-3501 .....</b>	<b>14</b>
<b>10 INITIAL SETUP WLM-3501 .....</b>	<b>14</b>
LOGIN PROCEDURE	14
<b>STATUS .....</b>	<b>15</b>
STATUS	15
STATISTICS	16
DHCP LIST	17
DIAGNOSTICS	18
<b>11 CONFIGURATION WIZARD .....</b>	<b>19</b>
<b>12 BASIC SETTINGS .....</b>	<b>20</b>
LAN SETTINGS	20
DHCP SETTINGS	21
WAN SETTINGS	22
SECURITY SETTINGS	27
WIRELESS ACL	29
<b>13 ADVANCED SETTINGS.....</b>	<b>30</b>
ADVANCES WIRELESS	30
QoS	32
UPnP	34
ROUTING	35
SNMP	36
DDNS	37
NAT	38
TR-69	39
<b>14 FIREWALL SETTINGS.....</b>	<b>40</b>
FIREWALL	40

ACL	41
IP FILTER	42
DMZ	45
VIRTUAL SERVER	46
<b>15 TOOLBOX SETTINGS</b>	<b>47</b>
PASSWORD	47
TIME SETTINGS	53
FIRMWARE UPGRADE	54
REBOOT	55

Revision 1.0  
© Sitecom Europe BV 2011

Note: All the information contained in this manual was correct at the time of publication.  
However, as our engineers are always updating and improving the product, your device's software may have a slightly different appearance or modified functionality than presented in this manual.

# Introduction

---

Congratulations on your purchase of the WLM-3501 Wireless ADSL2+ Modem. This modem is fully compliant with 802.11b, 802.11g and 802.11n. This modem provides the best performance when used in combination with 802.11n client adapters.

The WLM-3501 is not only a Modem or Wireless Access Point, but can also be used to connect wired Ethernet devices at 10/100 Mbit speeds.

For data protection and privacy, the WLM-3501 can encode all wireless transmissions with WEP, WPA or WPA2 encryption. By default, the modem is secured with a WPA2 (AES) encryption key. (The WPA2-key is printed on the label underneath the modem.)

With a built-in DHCP Server & powerful SPI firewall the WLM-3501 protects your computers against intruders and known Internet attacks, and also provides safe VPN pass-through.

With Sitecom Cloud Security, Sitecom goes one step further and ensures that you can surf the Internet even more safely, not only on your PC, but on all the devices in your home which you use to access the Internet. It does not matter whether you surf the Internet on a laptop, a tablet, a mobile telephone or your television. Thanks to the security that is integrated in the router, all the Internet devices in your home are protected against the dangers of Internet criminality.

# 1 Key Features

---

Features	Advantages
<b>IEEE 802.11g compliant</b>	Fully Interoperable with IEEE 802.11b / IEEE802.11g compliant devices
<b>Based on 802.11n technology</b>	WLM-3501: Up to 6 times faster than regular 802.11g  (in combination with a 150n or 802.11n wireless adapter)
<b>Four 10/100 Mbps Port (Auto-Crossover)</b>	To connect four wired PC's as well.
<b>Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI</b>	Avoids the attacks of Hackers or Viruses from Internet
<b>Supports 802.11i (WPA/WPA2, AES), VPN pass-through</b>	Provide mutual authentication (Client and dynamic encryption keys to enhance security)
<b>Integrated modem (Annex A)</b>	Fully compatible with the fastest ADSL2+ connections up-to-date.
<b>Sitecom Cloud Security</b>	Protect your home against cybercrime while browsing.

## 2 Package Contents

---

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

1. WLM-3501 modem/router
2. 110V~240V 12V 1A Power Adapter
3. Quick Install Guide
4. CD (User's Manual)
5. Warranty card
6. UTP cable
7. RJ11 cable

## 3 Cautions

---

This router's design and manufacturer has your safety in mind. In order to safely and effectively use this router, please read the following before usage.

### 3.1 Usage Cautions

The user should not modify this router. The environmental temperature should be within +5 ~ +35 degrees Celsius.

### 3.2 Power

The router's power voltage is DC 12V 1A.

When using this router, please connect the supplied AC adapter or AC adapter cable to the router's power jack. When placing the adapter cable, make sure it can not get damaged or be subject to pressure. To reduce the risk of electric shock, unplug the adapter first before cleaning it. Never connect the adapter to the router in a humid or dusty area. Do not replace the adapter or cable's wire or connector.

### 3.3 Repair

If the router has a problem, you should take it to an appointed repair centre and let the specialists do the repair. Never repair the router yourself, you might damage the router or endanger yourself.

### 3.4 Disposing of the Router

When you dispose of the router, be sure to dispose it appropriately. Some countries may regulate disposal of an electrical device, please consult with your local authority.

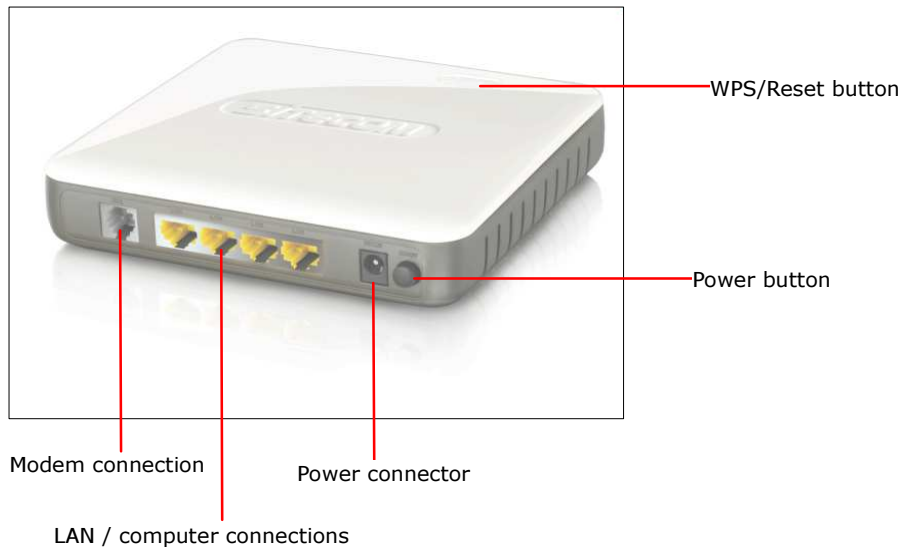
### 3.5 Others

When using this router, please do not let it come into contact with water or other liquids. If water is accidentally spilled on the router, please use a dry cloth to absorb the spillage. Electronic products are vulnerable, when using please avoid shaking or hitting the router, and do not press the buttons too hard.

- Do not let the router come into contact with water or other liquid.
- Do not disassemble the router, repair the router or change the design of the router, any damage done will not be included in the repair policy.
- Avoid hitting the router with a hard object, avoid shaking the router and stay away from magnetic fields.
- If during electrostatic discharge or a strong electromagnetic field the product will malfunction, unplug the power cable. The product will return to normal performance the next time it is powered on.

## 4 Product Layout

---

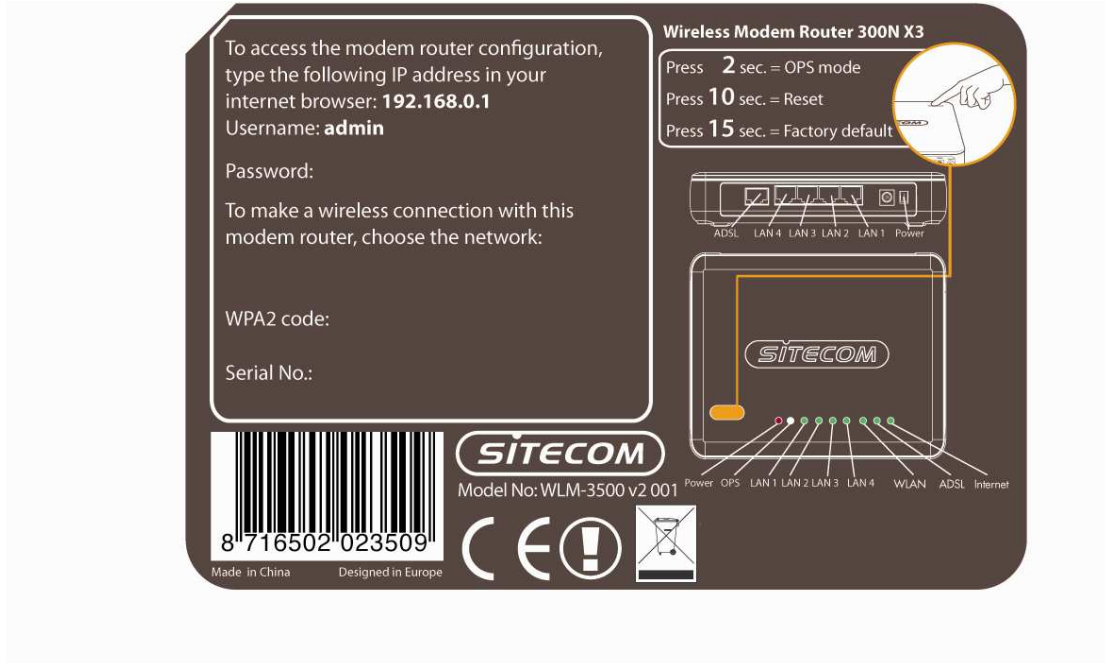


Port	Description
<b>ADSL</b>	Connect your telephone/ADSL cable this port
<b>LAN</b>	Connect the cable from your PC or network device to this ports.
<b>Power connector</b>	Connect your power adapter to this port.
<b>Power button</b>	Turn the modem On or Off.



## Back label

The back label describes the corresponding LED indications and port functionality.



LED	Description
<b>Power</b>	Lights up when powered ON. Blinks on TEST/RESET
<b>ADSL</b>	Lights up when an ADSL cable is connected.
<b>Internet</b>	Lights up when internet connection is UP.
<b>WLAN</b>	Lights up in Blue when WLAN is enabled. Blinks on traffic
<b>OPS</b>	Blinks when OPS mode is on
<b>LAN1~4</b>	When a LAN cable is connected the corresponding light lights up.

## 5 System Requirements

---

To begin using the WLM-3501, make sure you meet the following as minimum requirements:

- PC/Notebook.
- 1 Free Ethernet port.
- Wi-Fi card/USB dongle (802.11 b/g/n) – optional.
- Annex A, ADSL internet connection.
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera)
- Ethernet compatible CAT5 cables.

## 6 WLM-3501 Placement

---

You can place the WLM-3501 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Broadband Modem/Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and the ADSL/phone line should not be over 2 meters long.

## 7 Setup LAN, WAN

---



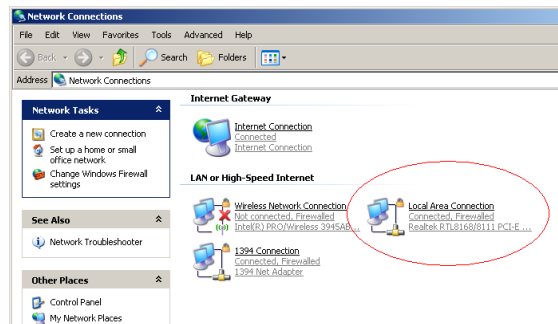
Modem connection

LAN / computer connections

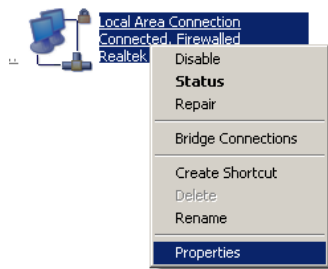
# 8 PC Network Adapter setup

## Windows XP

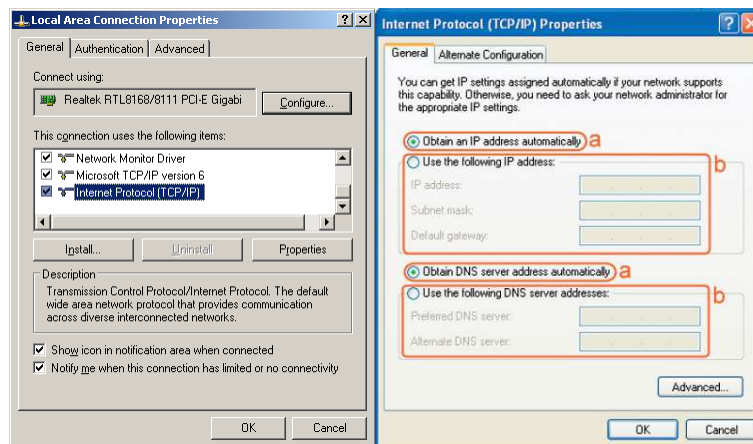
- Go to [Start Menu], → [Control panel], → [Network Connections].



- Right-mouse-click on the [Local Area Connection] icon, and select [properties]



- Select [Internet Protocol (TCP/IP)] =>Click [Properties].

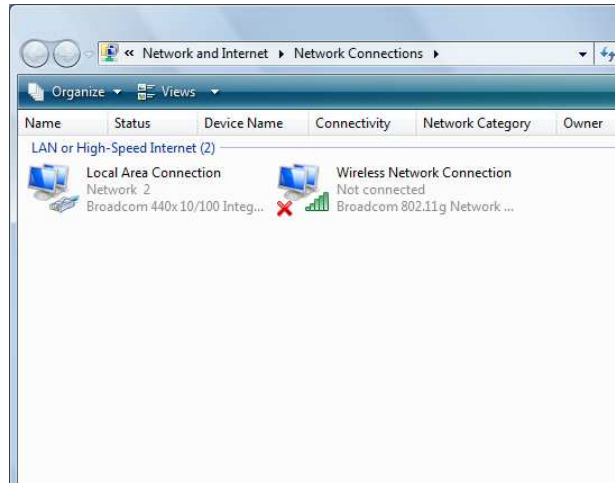


- Select the [General] tab.

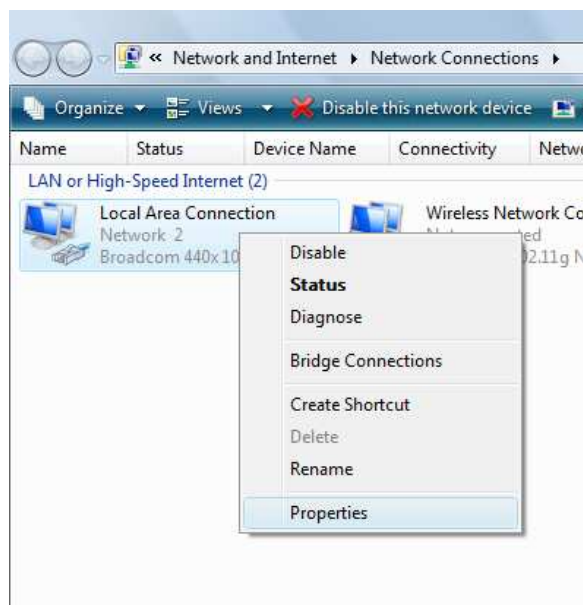
The WL-358/359 supports DHCP. Please select both [Obtain an IP address automatically] and [Obtain DNS server address automatically].

## Windows Vista/Windows 7

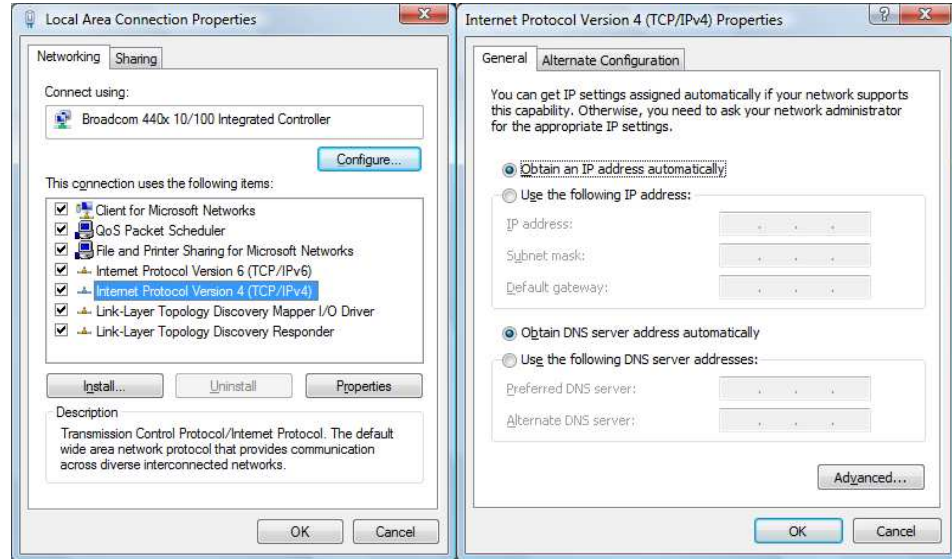
- Go to [Start Menu], → [Control panel], → [View network status and tasks], -> [Manage network connections].



- Right-mouse-click on the [Local Area Connection] icon, and select [properties]



- Select [*Internet Protocol Version 4 (TCP/IPv4)*], and Click [*Properties*].



- Open the [*General*] tab.

The WLM-3501 supports DHCP. Please select both [*Obtain an IP address automatically*] and [*Obtain DNS server address automatically*].

## 9 Bring up the WLM-3501

---

Connect the supplied power-adaptor to the power inlet port and connect it to a wall outlet. Press the Power-Button to turn the modem on.

The WLM-3501 automatically enters the self-test phase. During self-test phase, the Power LED will blink briefly, and then will be lit continuously to indicate that this product is in normal operation.

## 10 Initial Setup WLM-3501

---

### LOGIN procedure

1. OPEN your browser (e.g. Internet Explorer).



- 4 Type <http://192.168.0.1> in address bar and press [Enter]

Type user name and password (The default username is "admin", the password can be found on the back label of the device).



- 5 Click **OK**.
- 6 You will see the home page of the WLM-3501.

# Status

The pages in the status section provide you general information about the operational status of your device.

## Status

The System status section allows you to monitor the current status of your modem/router: the UP time, hardware information, serial number as well as firmware version information is displayed here. The page also shows extensive information concerning the ADSL status and current settings.

StatusStatisticsDHCP ListDiagnostics

ADSL Router Status

This page shows the current status and some basic settings of the device.

Firmware Version : 1.00

MAC Address : 00:AA:BB:01:23:45

LAN Configuration :

IP Address : 192.168.1.1

Subnet Mask : 255.255.255.0

DHCP Server : Enable

WAN Configuration :

Virtual Circuit : PVC 0

Status : Not Connected

Protocol : PPPoA

IP Address : N/A

Subnet Mask : N/A

Default Gateway : N/A

DNS Server : N/A

DSL :

ADSL Firmware Version : FwVer:3.16.1.0\_A\_TC3086 HwVer:T14.F7\_7.0

Operational Status : down

ADSL Modulation : N/A

Annex Mode : ANNEX A

Downstream

Upstream

SNR Margin (dB) : N/A N/A

Attenuation (dB) : N/A N/A

Data Rate : N/A N/A

# Statistics

You can view statistics on the processing of IP packets on the networking interfaces. You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems. To display statistics for any new data, click "Refresh".

The screenshot shows the web interface of a Sitecom wireless modem router 300N. The page is titled "Statistics" and displays network statistics for the selected interface, which is Ethernet. The statistics are organized into two columns: Transmit Statistics and Receive Statistics. A "REFRESH" button is located at the bottom right of the statistics area. The footer of the page contains the copyright information: "www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved".

Transmit Statistics		Receive Statistics	
Transmit Frames	8387	Receive Frames	2866
Transmitted Multicast Frames	1121	Received Multicast Frames	1061
Total bytes transmitted	3891479	Total bytes received	574251
Transmit Collision	0	Received CRC Errors	0
Transmit Error Frames	0	Received Under-size Frames	0



# DHCP List

This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client.

wireless  
**modem router** 300N  
SITCOM

Home Wizard Basic Settings Advanced Settings Firewall Toolbox Choose your language

Status Statistics **DHCP List** Diagnostics

**Active DHCP Clients table**

This table shows the assigned IP Address, corresponding MAC Address and expiration time of the connected clients.

#	Hostname	IP Address	MAC Address	Expiration time
0	rend-PC	192.168.1.100	00:26:22:AC:5F:2A	2 Days 23:58:39

www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved

# Diagnostics

The Diagnostics page allows you to test the current configuration. Click 'Start' to let the modem router perform several tasks to verify if the connection is operational.



## 11 Configuration Wizard

Click **Wizard** to configure the modem. The Setup wizard will now be displayed; check that the adsl line is connected and click **Next**.



Select your country from the Country list. Select your internet provider. Click **Next**.



Depending on the chosen provider, you may need to enter your user name and password or hostname in the following window. After you have entered the correct information, click **Next**.

Click **Finish** to complete the configuration.

# 12 Basic Settings

## LAN Settings

This page is used to configure the LAN interface of your ADSL Router. You can set IP address, subnet mask, and IGMP Snooping or modify the IPv6 address range .

wireless  
**modem router** 300N  
SITECOM

Home | Wizard | **Basic Settings** | Advanced Settings | Firewall | Toolbox | Choose your language ▾

LAN Settings | DHCP Settings | WAN Settings | Wireless settings | Security Settings | Wireless ACL

**LAN Settings**

This page is used to configure the LAN interface of your ADSL Router. Here you may change the setting for IP addresses, subnet mask, etc

IP Address :	192.168.1.1
Subnet Mask :	255.255.255.0
Alias IP Address :	192.168.2.1
Alias IP Subnet Mask :	255.255.255.0
IGMP Snooping :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Dynamic Route :	RIP1 ▾ Direction None ▾

**IPv6 Address**

IPv6 Address :	fe80::1	/	64
----------------	---------	---	----

SAVE CANCEL

www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved

# DHCP Settings

You can configure your network and the router to use the Dynamic Host Configuration Protocol (DHCP). This page allows you to select the DHCP mode that this router will support.

There are two different DHCP Modes: DHCP Server and DHCP Relay. When the router is acting as DHCP server, please configure the router in the "DHCP Server" page; while acting as DHCP Relay, you can setup the relay in the "DHCP Relay" page.

wireless

modem router<sup>300N</sup>

SITECOM

[Home](#) [Wizard](#) [Basic Settings](#) [Advanced Settings](#) [Firewall](#) [Toolbox](#) [Choose your language](#)

[LAN Settings](#) [DHCP Settings](#) [WAN Settings](#) [Wireless settings](#) [Security Settings](#) [Wireless ACL](#)

### DHCP Settings

This page is used to configure the DHCP Server and DHCP Relay settings.

DHCP Mode : ☐ None ☒ DHCP Server ☐ DHCP Relay configuration

Start IP :

IP Pool Count :

Max lease time :  Seconds (0 sets to the default value of 259200)

DNS Relay : ☒ Automatically ☐ Manually

Primary DNS :

Secondary DNS :

### Add DHCP Reservation

IP Address :

MAC Address :

#	IP Address	MAC Address	Drop
---	------------	-------------	------

### Radvd

Radvd : ☒ Disable ☐ Enable

### DHCPv6

DHCPv6 Server : ☒ Disable ☐ Enable

SAVE

CANCEL

www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved

# WAN Settings

This page allows you to manually configure the ADSL/WAN settings. The settings on this page require some knowledge concerning the WAN configuration we advice less-experienced users to configure the WAN settings using the Wizard (Chapter 10)

wireless

modem router 300N

SITECOM

[Home](#) | [Wizard](#) | **[Basic Settings](#)** | [Advanced Settings](#) | [Firewall](#) | [Toolbox](#) | [Choose your language](#)

[LAN Settings](#) | [DHCP Settings](#) | **[WAN Settings](#)** | [Wireless settings](#) | [Security Settings](#) | [Wireless ACL](#)

### WAN Settings

This page is used to configure basic WAN settings like ADSL and DNS settings

Virtual Circuit : PVC 0

PVCs Summary

Status : ☒ Enable ☐ Disable

VPI : 8 (range: 0-255)

VCI : 48 (range: 1-65535)

#### QoS

ATM QoS : ubr

PCR : 0 cells/second

SCR : 0 cells/second

MBS : 0 cells

#### IPv4/IPv6

IP Version : ☒ IPv4 ☐ IPv4/IPv6

#### Encapsulation

ISP : ☐ Dynamic IP Address  
☐ Static IP Address  
☒ PPPoA/PPPoE  
☐ Bridge Mode

#### PPPoE/PPPoA

Username : kpn

Password : ●●●

Encapsulation : PPPoA VC-Mux

#### Connection Setting

Connection : ☒ Always On (Recommended)  
☐ Connect on Demand(Close if idle for: minutes)  
☐ Connect Manually

TCP MSS Option : TCP MSS (0 means use default) 0 bytesbytes

#### IP Options

##### IP Common Options

Default route : ☒ Enable ☐ Disable

##### IPv4 Options

Get IP Address : ☐ Static ☒ Dynamic

Static IP : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway : 0.0.0.0

NAT : Enable

Dynamic Route : RIP1 Direction None

IGMP Proxy : ☐ Enable ☐ Disable

SAVE

### ATM VC

- **Virtual Circuit:** VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.
- **VPI:** The valid range for the VPI is 0 to 255. Enter the VPI assigned to you. This field may already be configured.
- **VCI:** The valid range for the VCI is 32 to 65535. Enter the VCI assigned to you. This field may already be configured.
- **ATM QoS:** Select **CBR** to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** for applications that are non-time sensitive, such as e-mail. Select **VBR** for burst traffic and bandwidth sharing with other applications.
- **PCR:** Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells.
- **SCR:** The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted.
- **MBS:** Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535

### Encapsulation:

- **ISP:** Select the encapsulation type your ISP uses from the **Encapsulation** list.  
Choices vary depending on what you select in the **Mode** field.  
If you select **Bridge** in the **Mode** field, select **1483 Bridged IP**.

If you select Routing in the Mode field, select PPPoA, 1483 Bridged IP, 1483 Router IP or PPPoE.

### PPPoE/PPPoA

- **User Name:** Enter the user name exactly as your ISP assigned.
- **Password:** Enter the password associated with the user name above.
- **Encapsulation:** select Bridge in the Mode field, select either PPPoA or RFC 1483.
- select Routing in the Mode field, select PPPoA, RFC 1483, ENET ENCAP or PPPoE.
- Multiplex: Select the method of multiplexing used by your ISP. Choices are VC or LLC.
- **Connection:** The schedule rule(s) have priority over your Connection settings.
- **Always on:** Select Always on Connection when you want your connection up all the time.
- **Connect on Demand:** Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field
- **Get IP Address:** Choose Static or Dynamic
- **Static IP Address:** Enter the IP address of ADSL Router in dotted decimal notation, for example, 192.168.1.254 (factory default).
- **IP Subnet Mask:** The default is 255.0.0.0. User can change it to other such as 255.255.255.0. Type the subnet mask assigned to you by your ISP (if given).
- **Gateway:** You must specify a gateway IP address (supplied by your ISP) when you use **1483 Bridged IP** in the **Encapsulation** field in the previous screen.

- **Network Address Translation:** Select **None**, **Many to One** or **Many to Many** from the drop-down list box. Refer to the NAT chapter for more details.
- **RIP Version:** Select the RIP version from RIP-1, RIP-2B and RIP-2M.
- **RIP Direction:** Select the RIP direction from None, Both, In Only and Out Only.
- **Multicast:** IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.



# Wireless Settings

This section provides the wireless network settings for your router. You can enable and configure the wireless AP function here.

wireless  
**modem router** 300N  
SITECOM

Home Wizard **Basic Settings** Advanced Settings Firewall Toolbox Choose your language ▼

LAN Settings DHCP Settings WAN Settings **Wireless settings** Security Settings Wireless ACL

**Wireless Basic Settings**

This page is used to configure the parameters for the wireless LAN like wireless encryption settings, channel and band

Access Point : ☒ Enable ☐ Disable

Channel : 01 Current Channel : 1

Wireless Mode : 802.11b+g+n

**11n Settings**

Channel Width : 20/40 MHz

Extension Channel : above the control channel

Guard Interval : Auto

MCS : Auto

**SSID Settings**

SSID index : 1

SSID : Sitecom

SAVE CANCEL

www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved

Parameter	Description
<b>Band</b>	Please select the radio band from one of the following options.  2.4GHz(B): 2.4GHz band, only allows 802.11b wireless network client to connect this router (maximum transfer rate 11Mbps).  2.4 GHz (G): 2.4GHz band, only allows 802.11g wireless network client to connect this router (maximum transfer rate 54Mbps).  2.4 GHz (B+G):2.4GHz band, only allows 802.11b and 802.11g wireless network client to connect this router (maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients).  2.4 GHz (N): 2.4GHz band, only allows 802.11n wireless network client to connect this router (maximum transfer rate 150Mbps).  2.4 GHz (G+N):2.4GHz band, only allows 802.11g and 802.11n wireless network client to connect this router (maximum transfer rate 54Mbps for 802.11g clients, and maximum 150Mbps for 802.11n clients).  2.4 GHz (B+G+N): 2.4GHz band, allows 802.11b, 802.11g, and 802.11n wireless network client to connect this router (maximum transfer rate 11Mbps

<b>Mode</b>	for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 150Mbps for 802.11n clients). It allows you to set the router to act in "AP", "Client" or "WDS" mode.
<b>SSID</b>	The SSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. The default SSID of the router is "default".
<b>Channel Width</b>	Set channel width of wireless radio. Do not modify default value if you don't know what it is, default setting is 'Auto 20/40 MHz'.
<b>Control Sideband</b>	Select the upper band or lower band for your radio frequency. While upper band is selected, the channel number you can select is from channel 5 to channel 11. While lower band is selected, the channel number you can select is from channel 1 to channel 7.
<b>Channel Number</b>	It is the radio channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel. Please select the country you are located and designate a channel that the router will use. If you want to let the router automatically to find an available channel with the highest signal strength, please select "Auto".
<b>Radio Power (mW)</b>	Set the maximum output power of the router. The higher output power, the wider coverage range.
<b>Associated Clients</b>	Click "Show Active Clients" button and you can see the wireless clients connected to the router.

---

When you finish, click 'Apply Changes' to save the settings made and restart the router so the settings will take effect after it reboots.

# Security Settings

This router provides complete wireless LAN security functions, include WEP, IEEE 802.1x, IEEE 802.1x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.

The screenshot shows the 'Security Settings' page for a Sitecom wireless modem router 300N. The page has a navigation bar with tabs: Home, Wizard, Basic Settings, Advanced Settings, Firewall, Toolbox, and a language dropdown. Below this is a sub-navigation bar with tabs: LAN Settings, DHCP Settings, WAN Settings, Wireless settings, Security Settings (selected), and Wireless ACL. The main content area is titled 'Wireless Security Settings' and includes a description: 'This page allows you to change WPS and security settings.' The settings are as follows: 'Use WPS' is set to 'Enable'; 'WPS Status' is 'Configured'; 'WPS mode' has 'PIN code' and 'PBC' options; 'WPS progress' is 'idle'. There are 'Start WPS' and 'Reset to OOB' buttons. Under the 'WPA-PSK' section, 'Authentication Type' is 'WPA2PSK', 'Encryption' is 'AES', and 'Pre-Shared Key' is 'sitecomtest' (with a note: '(8-63 characters or 64 Hex string)'). 'SAVE' and 'CANCEL' buttons are at the bottom right. A footer at the very bottom reads: 'www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved'.

Parameter	Description
<b>Encryption</b>	<p>You can choose "None" to disable the encryption or select "WEP", "WPA(TKIP)", "WPA2(AES)" or "WPA2 Mixed" mode for security. When "WEP" is enabled, please click "Set WEP Key" button to choose the default key and set the four sets of WEP keys.</p> <p><b>WEP</b> –WEP is less level of security than WPA. WEP supports 64-bit and 128-bit key lengths to encrypt the wireless data.</p> <p><b>WPA(TKIP)</b> – WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption. TKIP utilized a stronger encryption method and incorporates Message Integrity Code (MIC) to provide protection against hackers.</p> <p><b>WPA2(AES)</b> – WPA2, also known as 802.11i, uses Advanced Encryption Standard (AES) for data encryption. AES utilized a symmetric 128-bit block data encryption.</p> <p><b>WPA Mixed</b> – The router supports WPA (TKIP) and WPA2 (AES) for data encryption. The actual selection of the encryption methods will depend on the clients.</p>
<b>Use 802.1x Authentication</b>	<p>IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this wireless router before accessing the wireless LAN. The authentication is processed by a RADIUS server. Check this box to authenticates user by</p>

	IEEE 802.1x.
<b>WEP-64Bits</b>	WEP is less level of security than WPA. WEP supports 64-bit and 128-bit key lengths to encrypt the wireless data. The longer key length will provide higher security. When "WEP-64Bits" is selected, you have to enter exactly 5 ASCII characters ("a-z" and "0-9") or 10 hexadecimal digits ("0-9", "a-f") for each Key (1-4).
<b>WEP-128Bits</b>	When "WEP-128Bits" is selected, you have to enter exactly 13 ASCII characters ("a-z" and "0-9") or 26 hexadecimal digits ("0-9", "a-f") for each Key (1-4).
<b>WPA Authentication Mode</b>	There are two types of authentication mode for WPA. <b>Enterprise (RADIUS)</b> – It uses an external RADIUS server to perform user authentication. To use RADIUS, enter the IP address of the RADIUS server, the RADIUS port (default is 1812) and the shared secret from the RADIUS server. Please refer to "Authentication RADIUS Server" setting below for RADIUS setting.
<b>Pre-Shared Key Format</b>	<b>Personal (Pre-Shared Key)</b> – Pre-Shared Key authentication is based on a shared secret that is known only by the parties involved. To use WPA Pre-Shared Key, select key format and enter a password in the "Pre-Shared Key Format" and "Pre-Shared Key" setting respectively. You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key. For example: Passphrase: "iamguest" Hexadecimal Digits: "12345abcde"
<b>Pre-Shared Key Authentication RADIUS Server</b>	Please enter 8-63 characters as the "Pre-Shared Key". Enter the port (default is 1812), the IP address and the password of external RADIUS server are specified here.

When you finish, click '**save**' to save the settings made and restart the router so the settings will take effect after it reboots.

# Wireless ACL

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.



Parameter	Description
Active	Choose to either <b>Enable</b> – Enabled the Wireless Access Control <b>Disable</b> – Disable the Wireless Access Control
Actions	<b>Allow</b> – Only allow the wireless clients with the MAC Address you have specified can access to the router.  <b>Deny</b> – The wireless clients with the MAC Address you have specified will be denied accessing to the router.
MAC Address	Enter the MAC Address of the wireless clients for the filtering control.

When you finish, click '**save**' to save the settings made and restart the router so the settings will take effect after it reboots.

## 13 Advanced Settings

The advanced settings pages allow users to modify the more complex features of this device.

### Advances wireless

This page allows advanced users who have sufficient knowledge of wireless LAN. These setting shall not be changed unless you know exactly what will happen for the changes you made on your router.

The screenshot shows the 'Advanced Wireless' settings page for a Sitecom modem router 300N. The page has a navigation bar with tabs: Home, Wizard, Basic Settings, Advanced Settings (selected), Firewall, and Toolbox. Below the navigation bar, there are sub-tabs: Advanced Wireless (selected), QoS, UPnP, Routing, SNMP, DDNS, NAT, and TR-69. The main content area is titled 'Wireless Advanced Settings' and includes a warning: 'These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.' The settings are as follows:

Parameter	Value	Range
Beacon Interval	100	20~1000
RTS/CTS Threshold	2347	1500~2347
Fragment Threshold	2346	256~2346, even numbers only
DTIM	1	1~255
Broadcast SSID	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	

At the bottom right, there are 'SAVE' and 'CANCEL' buttons. The footer of the page reads: 'www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved'.

Parameter	Description
Beacon Interval	The interval of time that this wireless router broadcast a beacon. Beacon is used to synchronize the wireless network. The range for the beacon period is between 20 and 1024 with a default value of 100 (milliseconds).
Fragmentation Threshold	Fragment Threshold specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance. Enter a value from 256 to 2346.
RTS Threshold	This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset "RTS threshold" size, the RTS/CTS mechanism will not be enabled. The wireless router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

**DTIM****Broadcast SSID**

If this option is enabled, the router will automatically transmit the network name (SSID) into open air at regular interval. This feature is intended to allow clients to dynamically discover the router. If this option is disabled, the router will hide its SSID. When this is done, the clients cannot directly discover the router and **MUST** be configure with the SSID for accessing to the router. It is used to protect your network from being accessed easily.

When you finish, click '**save**' to save the settings made and restart the router so the settings will take effect after it reboots.

# QoS

QoS allows you to classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference ...etc. All the applications not specified by you are classified as rule name "Others". The rule with a smaller priority number has a higher priority; the rule with a larger priority number has a lower priority. You can adjust the priority of the rules by moving them up or down.

## Classification

wireless

modem router 300N

SITECOM

[Home](#) [Wizard](#) [Basic Settings](#) [Advanced Settings](#) [Firewall](#) [Toolbox](#) [Choose your language](#)

[Advanced Wireless](#) [QoS](#) [UPnP](#) [Routing](#) [SNMP](#) [DDNS](#) [NAT](#) [TR-69](#)

### Quality of Service

Configuration of classification table for IPQoS.

QoS : ☐ Enable ☒ Disable

Discipline : ☐ WRR ☒ Strict Priority

WRR weight : Highest: 8 High: 4 Medium: 2 Low: 1 [Discipline Save](#) [Rule&Action Summary](#)

Rule

Rule Index : 0

Active : ☐ Enable ☒ Disable

Application :

Physical Ports : ☐ eth0 ☐ eth1 ☐ eth2 ☐ eth3 ☐ ra0

Destination MAC Address :

IP Address :

Subnet Mask :

Port Range : ~

Source MAC Address :

IP Address :

Subnet Mask :

Port Range : ~

Protocol :

Vlan ID Range : ~

IPP/DS Field : ☐ IPP/TOS ☒ DSCP

IP Precedence Range : ~ ~

Type of Service :

DSCP Range : ~ ~ (Value Range: 0 - 63)

802.1p : ~ ~

Actions

IPP/DS Field : ☐ IPP/TOS ☒ DSCP

Remark :

Type of Service Remark :

DSCP Remark : (Value Range: 0 - 63)

802.1p Remark : ~ ~

Queue # :

[ADD](#) [DELETE](#) [CANCEL](#)

www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved



**Enable/Disable QoS** You can check "Enable QoS" to enable QoS functionality for the WAN port.

**Add a rule** Enter all the data required for the rule you wish to set and click Add to save this rule.

**Edit a QoS rule** Select the rule you want to edit and click "Edit", then enter the detail form of the QoS rule. Click "**Apply**" after editing the form and the rule will be saved.

**Discipline Save** allows to save the selected Qos discipline without changing the current rules.

**Rules&Action** summary provides an overview of the current effective Qos settings.

Click '**Add**' To save and apply the new rule.

# UPnP

When the UPnP function is enabled, the router can be detected by UPnP compliant system such as Windows 7. The router will be displayed in the Neighborhood of Windows 7, so you can directly double click the router or right click the router and select "Invoke" to configure the router through web browser.



Parameter	Description
<b>UPnP</b>	Enable or disable UPnP feature.
<b>Auto-configured</b>	This will allow Upnp enabled applications to open required ports in your router.

When you finish, click '**Save**' to save the settings made and restart the router so the settings will take effect after it reboots.

# Routing

The page enables you to define specific route for your Internet and network data.

Most users do not need to define routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN hosts and for the router provide the most appropriate path for all your Internet traffic.

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN.



Click 'Add route' to add a self defined router

Parameter	Description
<b>Destination IP Address</b>	The destination can be specified as the IP address of a subnet or a specific host in the subnet. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
<b>Subnet Mask</b>	The network mask of the destination subnet. The default gateway uses a mask of 0.0.0.0.
<b>Gateway IP address</b>	Gateway IP that should be used enter an address or select a pvc channel
<b>Metric</b>	Defines the number of hops between network nodes that data packets travel. The default value is 0, which means that the subnet is directly one hop away on the local LAN network.

When you finish, click '**Save**' to save the settings and restart the router so the settings will take effect after it reboots.

# SNMP

Simple Network Management Protocol (**SNMP**) is a troubleshooting and management protocol that uses the UDP protocol on port 161 to communicate between clients and servers. The router can be managed locally or remotely by SNMP protocol.

The screenshot shows the web interface of a Sitecom 300N wireless modem router. The top navigation bar includes links for Home, Wizard, Basic Settings, Advanced Settings (selected), Firewall, and Toolbox. Below this, a sub-menu shows Advanced Wireless, QoS, UPnP, Routing, SNMP (selected), DDNS, NAT, and TR-69. The main content area is titled 'SNMP Configuration' and contains a message: 'This page is used to configure the SNMP protocol.' Below this, there is a 'SNMP' section with two radio buttons: 'Enable' and 'Disable' (selected). There are also two text input fields labeled 'Get Community' and 'Set Community'. A 'SAVE' button is located at the bottom right of the configuration area. The footer of the page reads: 'www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved'.

Parameter	Description
<b>SNMP</b>	Select "Disable" or "Enable" to disable or enable the SNMP feature.
<b>Get Community</b>	Name of the read-only community. This read-only community allows read operation to all objects in the MIB.
<b>Set Community</b>	Name of the write-only community. This write-only community allows write operation to the objects defines as read-writable in the MIB.

When you finish, click '**Save**' to save the settings made and restart the router so the settings will take effect after it reboots.

# DDNS

Dynamic DNS (DDNS) allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers.

wireless  
**modem router** 300N  
SITECOM

Home Wizard Basic Settings **Advanced Settings** Firewall Toolbox Choose your language

Advanced Wireless QoS UPnP Routing SNMP **DDNS** NAT TR-69

**Dynamic DNS Configuration**  
This page is used to configure the Dynamic DNS address from DynDNS.org.

Dynamic DNS : ☐ Enable ☒ Disable

DDNS provider : www.dyndns.org

Hostname :

Username :

Password :

Wildcard support : ☐ Enable ☒ Disable

SAVE

www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved

Parameter	Description
<b>Enable</b>	Check the box to enable DDNS function.
<b>DDNS Provider</b>	Select your DDNS service provider here. This router supports DynDNS and TZO service providers
<b>Host Name</b>	Enter the domain name you've obtained from DDNS service provider.
<b>DynDns Settings</b>	
<b>Username</b>	Enter the username assigned by the DDNS service provider.
<b>Password</b>	Enter the password assigned by the DDNS service provider.
<b>Wildcard support</b>	Enable or disable the usage of wildcards (i.e. *.* )

When you finish, click '**Save**' to save the settings made and restart the router so the settings will take effect after it reboots.

# NAT

This page allows viewing or changing of the current status of the NAT for each VC.



Here it's possible to set Virtual server or DMZ settings for each virtual circuit. For more information about the DMZ and virtual server please read chapter **13 Firewall**.

## TR-69

As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework. In the course of the boom of the broadband market, the number of different Internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones). At the same time the configuration of this equipment became more complicated -- too complicated for the end-users. For this reason the TR-069 standard was developed. It provides the possibility of auto configuration of these access types. The technical specifications are managed and published by the Broadband Forum. Using TR-069, the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically. Accordingly other service functions can be provided. TR-069 is the current standard for activation of terminals in the range of DSL broadband market.

The screenshot displays the web interface of a Sitecom wireless modem router 300N. The top navigation bar includes links for Home, Wizard, Basic Settings, Advanced Settings (selected), Firewall, and Toolbox. A language selection dropdown is also present. Below the navigation bar, a sub-menu highlights various configuration options: Advanced Wireless, QoS, UPnP, Routing, SNMP, DDNS, NAT, and TR-69 (selected). The main content area is titled "CWMP Setup" and contains the following sections:

- CWMP Setup:** A section with the text "This page is used to configure TR-069." and a radio button to "Enable" CWMP.
- ACS Login Information:** Fields for "URL" (http://122.193.99.166:80/entry\_basic/node1/tr069), "Username" (basic), and "Password" (basic).
- Connection Request Information:** Fields for "Path" (/tr069), "Username" (123), and "Password" (123).
- Periodic Inform Config:** A radio button to "Enable" periodic inform configuration and an "Interval" field set to 5000.

At the bottom right of the form are "APPLY" and "CANCEL" buttons. The footer of the page contains the text: "www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved."

# 14 Firewall Settings

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

## Firewall



Parameter	Description
Firewall	Enable or Disable the firewall
SPI	Enable or Disable the firewall (Warning: If you enable SPI, all traffic initiated from WAN will be blocked)



# ACL

This page is used to IP addresses for Access Control. If ACL is enabled only the IP Addresses that are in the ACL Table can access the CPE.

The screenshot shows the 'ACL Configuration' page of a Sitecom modem router 300N. The page has a navigation bar with 'Home', 'Wizard', 'Basic Settings', 'Advanced Settings', 'Firewall', and 'Toolbox'. The 'Firewall' tab is selected, and the 'ACL' sub-tab is active. The page title is 'wireless modem router 300N'. The 'ACL Configuration' section includes a description: 'This page is used to configure the IP Address for Access Control List. If ACL is enabled, just these IP address that in the ACL Table can access CPE. Here you can add/delete IP Address.' The configuration options are: 'ACL' (radio buttons for 'Enable' and 'Disable', with 'Disable' selected), 'ACL Rule Index' (a dropdown menu showing '1'), 'Active' (radio buttons for 'Yes' and 'No', with 'Yes' selected), 'Secure IP Address' (two text boxes with '0.0.0.0' and '~ 0.0.0.0', with a note '(0.0.0.0 - 0.0.0.0 means all IPs)'), 'Application' (a dropdown menu showing 'ALL'), and 'Interface' (a dropdown menu showing 'Both'). Below these settings is an 'ACL Table' with the following data:

Index	Active	Secure IP Address	Application	Interface
1	0.0.0.0~0.0.0.0	ALL	Both	

At the bottom of the page are buttons for 'SET', 'DELETE', and 'CANCEL'. The footer text is 'www.sitecom.com | © 1996 - 2011 Sitecom Europe BV; all rights reserved'.

**ACL** Enable or disable Access Control

**ACL Rule index** Select an index number for the rule you are creating.

**Active** Select if the Rule should be active or not

**Secure IP Address** Enter the range IP addresses for which this rule should be effective.

**Application** Select an application from the list or choose 'all'.

**Interface** Select the interface for this rule, 'WAN' or 'LAN'.

# IP Filter

wireless  
**modem router** 300N  
SITECOM

Home Wizard Basic Settings Advanced Settings **Firewall** Toolbox Choose your language ▾

Firewall **ACL** **IP Filter** DMZ Virtual Server

**Filter**  
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

**Filter Type**  
Filter Type Selection: IP/MAC Filter ▾

**Rule Type**  
Rule Type Selection: White List ▾

**IP/MAC Filter Rule Editing**  
IP/MAC Filter Rule Index: 1 ▾

Active: ☐ Enable ☒ Disable

Interface: PVC0 ▾

Direction: Both ▾

Rule Type: IP ▾

Source IP: 0.0.0.0 (0.0.0.0 for all)

Subnet Mask: 0.0.0.0

Port Number: 0 (0 for all)

Destination IP: 0.0.0.0 (0.0.0.0 for all)

Subnet Mask: 0.0.0.0

Port Number: 0 (0 for all)

Protocol: TCP ▾

**IP / MAC Filter Listing**

#	Active	Interface	Direction	Source Address/Mask	Destination Address/Mask	MAC Address	Src Port	Dst Port	Protocol
1	No	\$Interface	Both	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0		0	0	TCP

SET DELETE CANCEL

www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved

## Filter Type

Choose the type of filter you wish to use, there are 3 possible types of filter .

- IP/Mac Filter
- Application filter
- URL block

## IP Filter Rule Editing

- **IP Filter Rule Index:** This is item number
- **Active:** Select **Yes** from the drop down list box to enable IP filter rule.
- **Source IP Address:** The source IP address or range of packets to be monitored.
- **Subnet Mask:** It is the destination IP addresses based on above destination subnet IP
- **Source Port Number:** This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535**. It is recommended that this option be configured by an advanced user.

- **Destination IP Address:** This is the destination subnet IP address.
- **Subnet Mask:** It is the destination IP addresses based on above destination subnet IP
- **Destination Port Number:** This is the Port or Port Ranges that defines the application.
- **Protocol:** It is the packet protocol type used by the application, select either **TCP** or **UDP** or **ICMP**
- **Rule Unmatched:** Select action for the traffic unmatching current rule; Forward to leave it pass through, and NEXT to check it by the next rule.

#### **IP Filter Listing**

- **#:** Item number.
- **Active:** Whether the connection is currently active.
- **Src IP Mask:** The source IP address or range of packets to be monitored.
- **Dest IP Mask:** This is the destination subnet IP address.
- **Src port:** This Port or Port Ranges defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535**. It is recommended that this option be configured by an advanced user.
- **Dest Port:** This is the Port or Port Ranges that defines the application.
- **Protocol:** It is the packet protocol type used by the application, select either **TCP** or **UDP** or **ICMP**

## Application filter

Here you can choose which applications should be blocked or allowed access.



Choose which application should be allowed or denied access and click '**Save**' to apply the settings.

## The URL block

Here it's possible to block certain websites.



## Filter type

Enter the website you wish to block and make sure the rule is active. Click '**Save**' to apply the new rule.

## URL Filter Listing

Shows all entered URL block rules.

# DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP Address as the DMZ Host, all incoming packets will be checked by the firewall and NAT algorithms then passed to the DMZ Host.

For example, if you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host.



Enable DMZ and enter the IP address for which you want unrestricted access to the internet in the **DMZ Host IP address**. Click Apply to save and apply the settings.

# Virtual server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number.

The screenshot shows the 'Virtual Server' configuration page of a Sitecom modem router 300N. The page has a navigation bar with tabs: Home, Wizard, Basic Settings, Advanced Settings, Firewall, and Toolbox. The 'Firewall' tab is selected, and within it, the 'Virtual Server' sub-tab is active. The page title is 'Virtual Server'. Below the title, there is a description: 'The Virtual Server rule index for this VC. You can specify upto 10 rules. All the VCs with single IP will use the same Virtual Server rules.' Below this, there is a form to add a new rule. The form has four fields: 'Virtual Server for : Single IP's Account/PVCO', 'Start Port : 1', 'End Port : 9678', and 'Local IP Address : 192.168.1.105'. Below the form, there is a table titled 'Virtual Server Listing' with columns: Rule, Start Port, End port, Local IP Address, Edit, and Drop. The table contains 10 rows, with the first row (Rule 0) showing the current rule configuration. The other rows (Rules 1-9) show 'N/A' for Start Port, End port, and Local IP Address, and an 'Edit' icon for each. At the bottom of the page, there are buttons for 'APPLY', 'BACK', and 'CANCEL'. The footer of the page contains the text: 'www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved.'

Rule	Start Port	End port	Local IP Address	Edit	Drop
0	1	9678	192.168.1.105		
1	N/A	N/A	N/A		
2	N/A	N/A	N/A		
3	N/A	N/A	N/A		
4	N/A	N/A	N/A		
5	N/A	N/A	N/A		
6	N/A	N/A	N/A		
7	N/A	N/A	N/A		
8	N/A	N/A	N/A		
9	N/A	N/A	N/A		

**Local IP** This is the LAN client/host IP address that the Public Port number packet will be sent to.

**Start port** Here the starting port number must be entered

**End port** Here the end port number must be entered

Note : The ports from the start port till the End port will be opened

Click the 'edit icon' to change an existing rule.

Click '**Apply**' for the changes to take effect.

# 15 TOOLBOX Settings

---

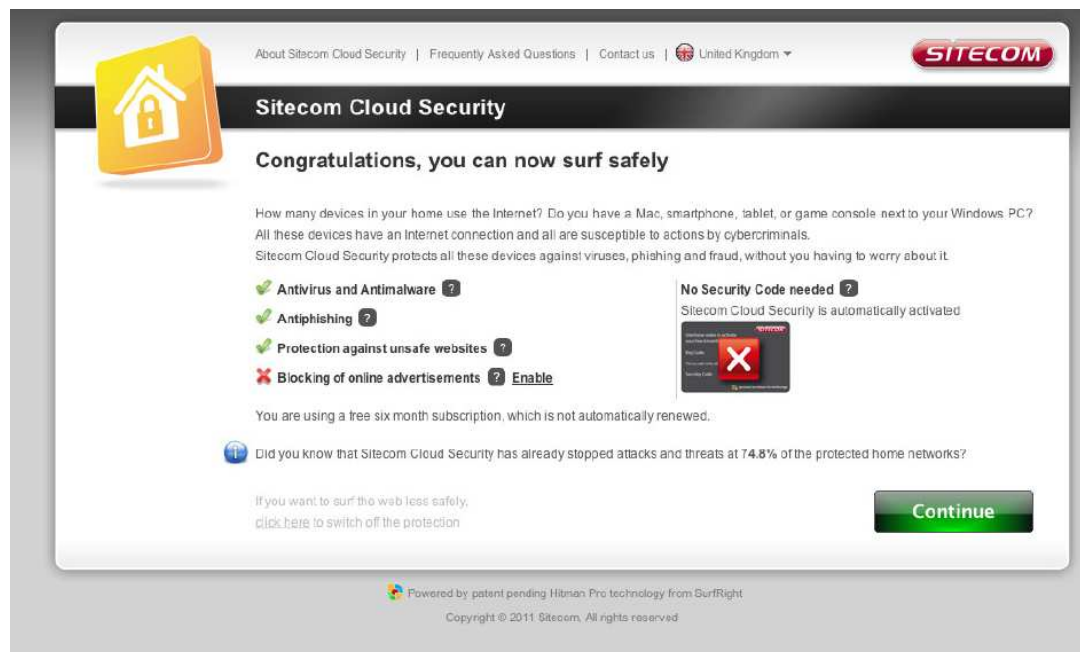
## Sitecom Cloud Security

Antivirus software alone is not safe enough. You can now benefit from additional built-in security in your modem or router. Protect all devices in your home network against cybercrime while browsing. Activated automatically, your network and devices are better secured than ever before.

Your Sitecom device comes with a 6 month free *Sitecom cloud security* subscription.

After you have set up your Sitecom device for internet access, open the webbrowser and enter <http://www.sitecomcloudsecurity.com> in the address bar.

If the device has been properly configured the following web page should be shown.

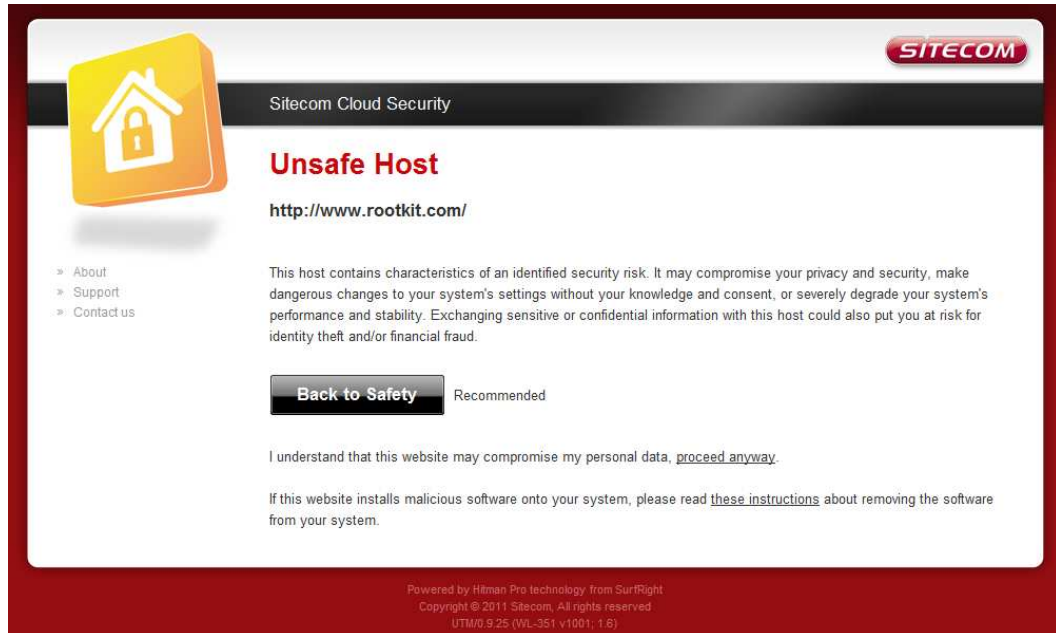


Here you can see which security features are activated.

The *Sitecom Cloud Security* service offers the following protection options:

- Anti-Malware
- Anti-Phishing
- Protection against unsafe websites
- Advertisement blocking

With the protection of *unsafe websites* activated the *Sitecom Cloud Security* will always check if a website is safe. If it is not safe it will inform you that is not safe to enter.

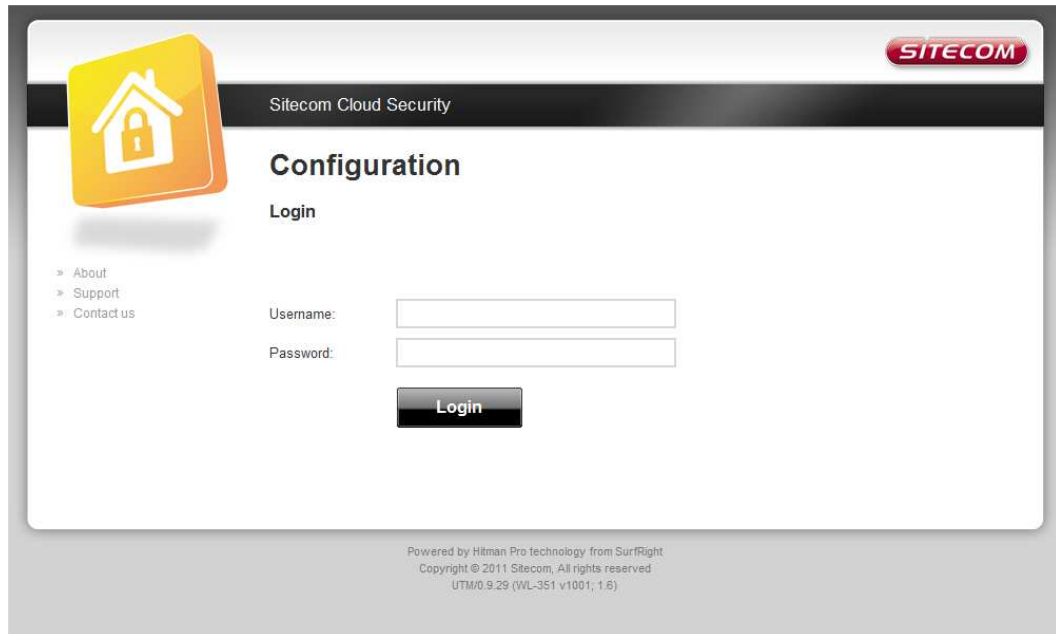


If you still wish to visit this webpage click on 'proceed anyway'. Alternatively click 'Back to Safety' so that your security will not be breached.



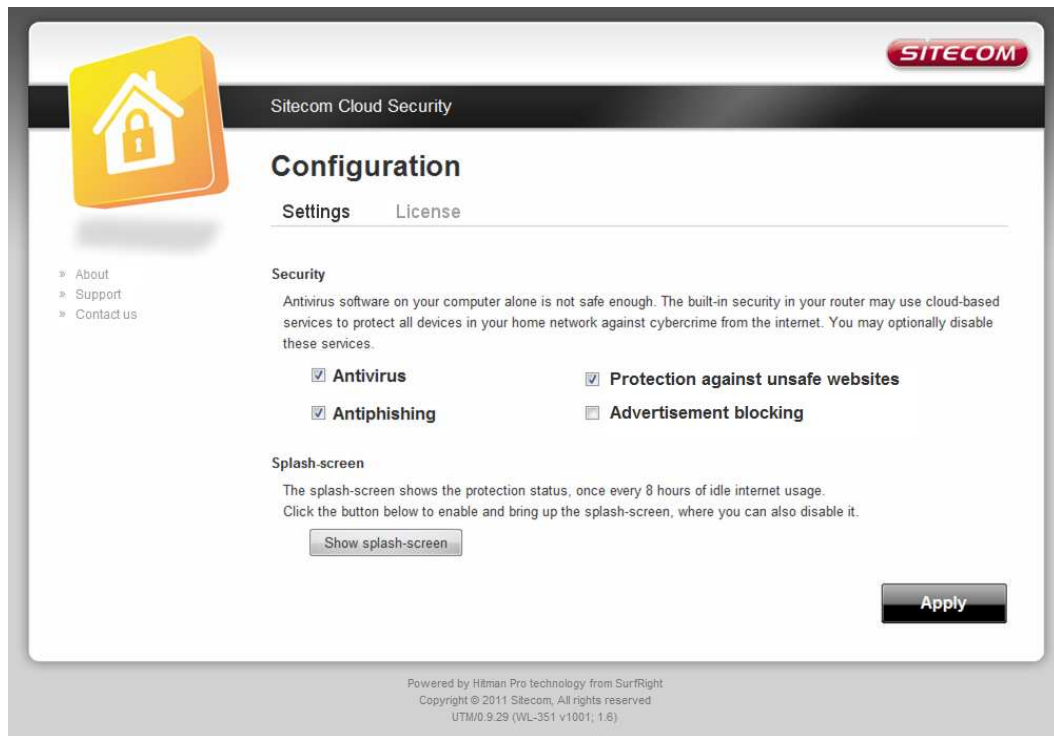
If you wish to change your security options or to extend your subscription at any time, open <http://www.sitecomcloudsecurity.com> from your web browser.

You will be asked for a username and password. These can be found on the backlabel on the bottom of your Sitecom router or modem.

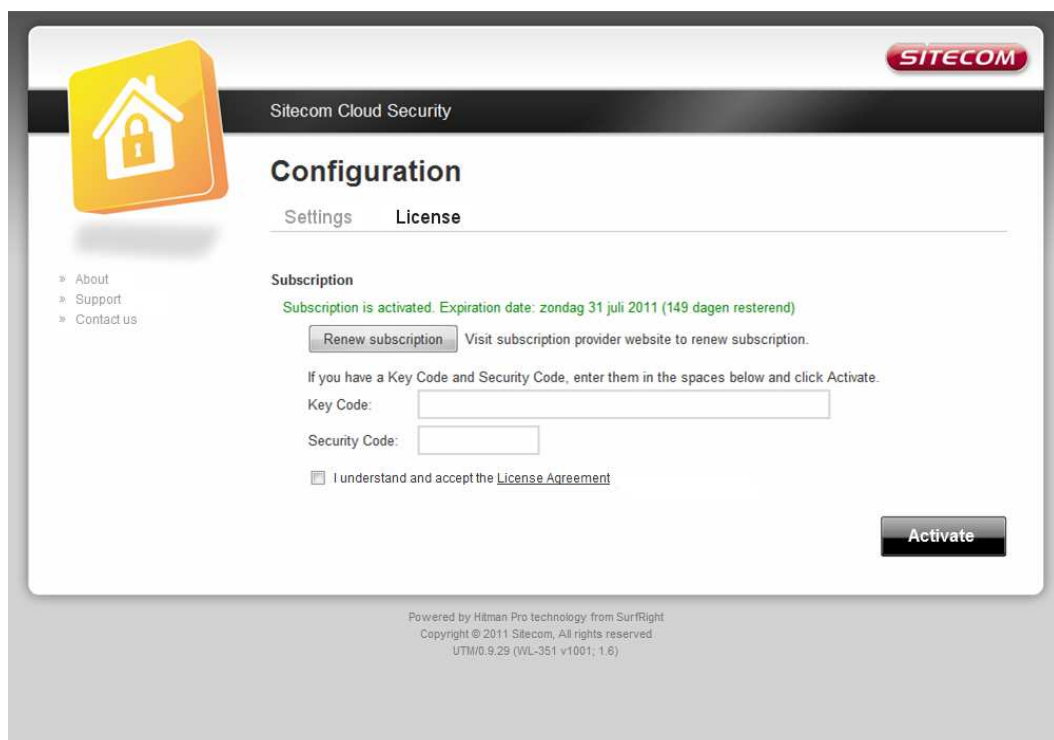


The screenshot displays the 'Sitecom Cloud Security' configuration interface. At the top left is a yellow house icon with a padlock. The top right features the 'SITECOM' logo. Below the logo, the text 'Sitecom Cloud Security' is visible. The main heading is 'Configuration', followed by a 'Login' section. On the left, there are links for 'About', 'Support', and 'Contact us'. The login form consists of 'Username:' and 'Password:' labels, each followed by a text input field. A 'Login' button is positioned below the password field. At the bottom, fine print states: 'Powered by Hitman Pro technology from SurfRight', 'Copyright © 2011 Sitecom, All rights reserved', and 'UTM/0 9.29 (WL-351 v1001; 1.6)'.

If the login succeeded you can click on 'Settings' to change your security options.



Or click 'License' to renew your subscription.



If you wish to disable Sitecom cloud security at any time, open the webpage of your Sitecom product and log in with the supplied credentials (these can be

found on the back label on the bottom of your Sitecom device).

Go to Toolbox and select "Sitecom Cloud Security".



Click the "Disable" radio button and click 'Apply' for the settings to take effect.

## Password

This page allows you to set the password to access the web server of the router.



If the password you typed in 'New Password' and 'Confirmed Password' field are not the same, you'll see the following message:

"Please retype the new password again when you see above message."

If the current and new passwords are correctly entered, after you click 'Apply', you'll be prompted to input your new password:



A Windows-style dialog box titled "Connect to 192.168.2.1". The title bar is blue with a question mark icon and a close button (X). Below the title bar is a blue header area with a yellow key icon. The main area has a light beige background. It displays "Default: admin/1234". Below this are two input fields: "User name:" with a dropdown menu showing a user icon, and "Password:" with a text box. A checkbox labeled "Remember my password" is below the password field. At the bottom are "OK" and "Cancel" buttons.

Connect to 192.168.2.1

Default: admin/1234

User name:

Password:

☐ Remember my password

OK Cancel

Please use new password to enter web management interface again, and you should be able to login with new password.

# Time Settings

The Time Zone allows your router to set its time; especially for recording System Log.

The screenshot shows the 'Time Zone Setting' page of a Sitecom 300N wireless modem router. The page has a header with the router's name and a navigation bar with tabs: Home, Wizard, Basic Settings, Advanced Settings, Firewall, and Toolbox. Below the navigation bar, there are sub-tabs: Sitecom Cloud Security, Password, Time Settings (selected), Firmware, and Reboot. The main content area is titled 'Time Zone Setting' and includes a description: 'You can maintain the system time by synchronizing with a public time server over the Internet.' The 'Current Time' is shown as 'N/A (Can't find NTP server)'. Under 'Time Synchronization', there are three radio buttons: 'NTP Server automatically' (selected), 'PC's Clock', and 'Manually'. Below this, there is a 'Time Zone Select' dropdown menu showing '(GMT+08:00) Beijing, Hong Kong, Perth, Singapore, Taipei'. There are also 'Daylight Saving' radio buttons for 'Enable' and 'Disable' (selected). At the bottom, there is an 'NTP Server Address' field with the value '0.0.0.0' and a note '(0.0.0.0: Default Value)'. 'SAVE' and 'CANCEL' buttons are at the bottom right. A footer at the very bottom reads 'www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved'.

Parameter	Description
<b>Current Time</b>	The current time of the specified time zone. You can set the current time by yourself or configured by SNTP server.
<b>Time Zone Select</b>	Select the time zone of the country you are currently in. The router will set its time based on your selection.
<b>Enable SNTP client update</b>	Check the box to enable router to update time from SNTP server.
<b>SNTP server</b>	The IP address or the host name of the SNTP server. You can select from the list or set it manually.

When you finish, click '**Save**'.  
The router so the settings will take effect after it reboots.

# Firmware Upgrade

The screenshot shows the web interface of a Sitecom wireless modem router 300N. The page is titled "Firmware upgrade" and contains the following elements:

- Navigation Bar:** Home, Wizard, Basic Settings, Advanced Settings, Firewall, Toolbox. A "Choose your language" dropdown is on the right.
- Sub-Menu:** Sitecom Cloud Security, Password, Time Settings, **Firmware**, Reboot.
- Firmware upgrade section:**
  - Text: "On this page you can upgrade the routers firmware to a newere version (when available)"
  - Form: "enable automatic firmware update" with radio buttons for "Enable" (selected) and "Disable".
  - Form: "New Firmware Location" with radio buttons for "romfile" and "tclinux.bin".
  - Form: "New Firmware Location" with a text input field and a "Bladeren..." button.
  - Form: "Romfile Backup" with a "ROMFILE BACKUP" button.
  - Form: "Status" with a text input field.
- Upgrade Button:** A button labeled "UPGRADE" at the bottom right.
- Footer:** "Thist might take several minutes, don't power off the router during uprade. The router will restart after the uprade." and "www.sitecom.com | © 1996 - 2011 Sitecom Europe BV, all rights reserved".

**Enable Automatic firmware update** When enabled the router will check for updates on the firmware if an updated firmware has been released the router will inform you that a newer firmware is available and offers to download and install the firmware.

This page also allows you to manually upgrade the firmware for the router. Click "Browse" button to select the firmware file and click "Upload" button to start upgrading.

**Romfile backup** Allows saving all current settings to a file.

**IMPORTANT!** Do not turn off your router while this procedure is in progress.

# Reboot

Whenever you use the Web configuration to change system settings, the changes are initially placed in temporary storage. To save your change for future use, you have to click "Apply" to reboot the router. If you have encountered problems during the configuration, you can click the "OPS" button in the top panel of the router over 15 seconds to reset default settings.

